Computer Hacking Forensic Investigator

Varighet: 5 Days   Kurskode: CHFI

Beskrivelse:

EC-Council releases the most advanced Computer Forensic Investigation program in the world. CHFIv8 presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.
Battles between corporations, governments, and countries are no longer fought using physical force. Cyber war has begun and the consequences can be seen in every day life. With the onset of sophisticated cyber-attacks, the need for advanced cyber security and investigation training is a mandate in the present day. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminals, then this is the course for you. This course helps students to excel in digital evidence acquisition, handling and analysis in a forensically sound manner. Acceptable in a court of law, these skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats and other intricate cases involving computer systems.

Målgruppe:

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

Agenda:

- During this EC-Council Computer Hacking Forensic Investigator course delegates will learn will learn how to create an effective computer crime policy and how to implement this policy effectively.

- After attending our Computer Hacking Forensics Investigator Training, you will leave with an applicable computer forensics toolkit that will enable you to perform a legally admissible forensics investigation and the skills to run the investigation properly.

- This hands-on computer forensics training offers practical experience in a wide array of computer forensics situations that are applicable to the real world. Learn everything relating to computer forensics --- from how to establish a proper chain of custody that is admissible in a court of law to recovering files from intentionally damaged media.

Forkunnskaper:

It is strongly recommended that you attend the CEH class before enrolling into CHFI program.

- CHE- Certified Ethical Hacker v8

Test og sertifisering

-

Innhold:

- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation

- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems

- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData

- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK

- FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Computer Forensics Investigation Process
- Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks

- Foresics Investigation using EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing And Event Correlation
- Network Forensics, Investigation Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

Ytterligere informasjon:

For mer informasjon eller kursbooking, vennligst ring oss 22 95 66 00

info@globalknowledge.no

www.globalknowledge.no

Grenseveien 97, 0663 Oslo, PO Box 6256 Etterstad, 0606 Oslo, Norway